Attorney Docket No. 1032326-000292

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

OIPE IAP13 MAR 29 2006 PATENT & TRADEMARK OFFICE

In re Patent Application of	
Jean-Sebastien Coron et al.	Group Art Unit: 2131
Application No.: 10/522,420	Examiner:
Filed: July 26, 2005	Confirmation No.: 5656
For: A DATA ENCIPHERING METHOD AND ASSOCIATED CRYPTOGRAPHIC SYSTEM AND ASSOCIATED COMPONENT (As Amended)	

REQUEST FOR CORRECTED OFFICIAL FILING RECEIPT

Commissioner for Patents
Office of Initial Patent Examination
Customer Service Center
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Enclosed is a copy of the Official Filing Receipt marked in red to show correction that is needed. The correction is as follows:

Please correct the title to - -A DATA ENCIPHERING METHOD AND ASSOCIATED CRYPTOGRAPHIC SYSTEM AND ASSOCIATED COMPONENT- -.

Issuance of a corrected Official Filing Receipt is respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: March 29, 2006

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPL NO.	FILING OR 371 (c) DATE	ART UNIT	FIL FEE REC'D	ATTY.DOCKET NO	DRAWINGS	TOT CLMS	IND CLMS
10/522,420	07/26/2005	2131	1030	032326-292		11	3

CONFIRMATION NO. 5656

21839
BUCHANAN INGERSOLL PC
(INCLUDING BURNS, DOANE, SWECKER & MATHIS)
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

FILING RECEIPT

OC000000018205049

OIPE IAP13
MAR 29 2006
PATENT & TRADEMARK OFFICE

Date Mailed: 03/20/2006

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Jean-Sebastien Coron, Paris, FRANCE;
Marc Joye, Saint Zacharie, FRANCE;
David Naccache, Paris, FRANCE;
Pascal Paillier, Paris, FRANCE;

Assignment For Published Patent Application

GEMPLUS, Gemenos, FRANCE

Power of Attorney: The patent practitioners associated with Customer Number **21839**.

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/FR03/02364 07/25/2003

Foreign Applications

FRANCE 02/09475 07/26/2002

NAU/PAU
MAR 27 2006

Projected Publication Date: To Be Determined - pending completion of Security Review

Non-Publication Request: No

Early Publication Request: No

BUCHANAN INGERSOLL PC
MAR 23 2006
DOCKETED 3-24-06 EH

032326-00092
JAL/NEW

Title Data ~~encryption~~ enciphering / and associated method cryptographic system and associated component

Preliminary Class

380

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

OIPE IAP13 MAR 29 2006 PATENT & TRADEMARK OFFICE

43

PCT Postcard

Applicant/ Inventor: Jean-Sebastien Coron et al. **Appln. No.:**

Docket No.: 032326-292 **Working Atty.:** James A. LaBarre / rsc **Date:** January 26, 2005

Title: A DATA ENCIPHERING METHOD AND ASSOCIATED CRYPTOGRAPHIC SYSTEM AND COMPONENT (As Amended)

Dkt. Clerk Initials

The following was/were received in the U.S. Patent and Trademark Office on the date stamped hereon:

- ☐ Transmittal Letter to the U.S. Receiving Office/ Response to Invitation (PTO-1382)
- ☒ Transmittal Letter to U.S. Designated/Elected Office (DO/EO/US) Concerning Filing Under 35 USC 371 (PTO-1390)
- ☐ PCT Request (PCT/RO/101) ( ) pgs.

INCLUDING:

- ☒ Specification (pages 1 - 10)
- ☒ Claims (claims(s) 1 - 10 , 4 pgs.)
- ☐ Drawings (Fig(s). 1 - , pgs.)
- ☐ Abstract of the Disclosure
- ☐ PCT Fee Calculation Sheet Annex to the Request (PCT/RO/101 (Annex))
- ☐ PCT Demand (PCT/IPEA/401) International Preliminary Examination Report
- ☐ PCT Fee Calculation Sheet Annex to Demand for Int'l. Preliminary Exam. (PCT/IPEA/401 (Annex))
- ☐ PCT Notice of Confirmation of Precautionary Designations (PCT/RO/144)
- ☐ Executed Declaration/Power of Attorney
- ☐ Unexecuted Declaration/Power of Attorney
- ☐ Assignment/Assignment Recordation Form Cover Sheet (PTO-1595)
- ☐ Appointment of Agent
- ☒ Preliminary Amendment
- ☐ Information Disclosure Statement Transmittal
- ☒ Information Disclosure Citation (PTO-1449)
- ☒ Information Disclosure Statement w/ 0 document(s)
- ☒ Patent Application Data Sheet
- ☒ Gen. Authorization for Petition for Ext. of Time and Payment of Fees
- ☐ Diskette
- ☐ Check for $ is enclosed
- ☐ Check for $ is enclosed
- ☐ Charge $ to Deposit Account
- ☒ Charge $ 1,000.00 to credit card. Form PTO-2038 is attached.
- ☒ PCT/ISA/210
- ☐
- ☐
- ☐

OIPE JC174 JAN 26 2005 PATENT & TRADEMARK OFFICE

If submitting documents via Express Mail, provide the Express Mailing Label No. below:

Express Mail Mailing Label No.

PCT Postcard

Applicant/ Inventor: Jean-Sebastien Coron et al. 10/522420 PT07 Rec'd PCT/PTO 26 JAN 2005 **Appln. No.:**

Docket No.: 032326-292 **Working Atty.:** James A. LaBarre / rsc **Date:** January 26, 2005

Title: A DATA ENCIPHERING METHOD AND ASSOCIATED CRYPTOGRAPHIC SYSTEM AND COMPONENT (As Amended)

Dkt. Clerk Initials

The following was/were received in the U.S. Patent and Trademark Office on the date stamped hereon:

- ☐ Transmittal Letter to the U.S. Receiving Office/ Response to Invitation (PTO-1382)
- ☒ Transmittal Letter to U.S. Designated/Elected Office (DO/EO/US) Concerning Filing Under 35 USC 371 (PTO-1390)
- ☐ PCT Request (PCT/RO/101) ( ) pgs.

INCLUDING:

- ☒ Specification (pages 1 - 10)
- ☒ Claims (claims(s) 1 - 10 , 4 pgs.)
- ☐ Drawings (Fig(s). 1 - , pgs.)
- ☐ Abstract of the Disclosure
- ☐ PCT Fee Calculation Sheet Annex to the Request (PCT/RO/101 (Annex))
- ☐ PCT Demand (PCT/IPEA/401) International Preliminary Examination Report
- ☐ PCT Fee Calculation Sheet Annex to Demand for Int'l. Preliminary Exam. (PCT/IPEA/401 (Annex))
- ☐ PCT Notice of Confirmation of Precautionary Designations (PCT/RO/144)
- ☐ Executed Declaration/Power of Attorney
- ☐ Unexecuted Declaration/Power of Attorney
- ☐ Assignment/Assignment Recordation Form Cover Sheet (PTO-1595)
- ☐ Appointment of Agent
- ☒ Preliminary Amendment
- ☐ Information Disclosure Statement Transmittal
- ☒ Information Disclosure Citation (PTO-1449)
- ☒ Information Disclosure Statement w/ 0 document(s)
- ☒ Patent Application Data Sheet
- ☒ Gen. Authorization for Petition for Ext. of Time and Payment of Fees
- ☐ Diskette
- ☐ Check for $ is enclosed
- ☐ Check for $ is enclosed
- ☐ Charge $ to Deposit Account
- ☒ Charge $ 1,000.00 to credit card. Form PTO-2038 is attached.
- ☒ PCT/ISA/210
- ☐
- ☐
- ☐

If submitting documents via Express Mail, provide the Express Mailing Label No. below:

Express Mail Mailing Label No.

OIPE IAP13
MAR 29 2006
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	Group Art Unit: Unassigned
Jean-Sebastien CORON et al.	Examiner: Unassigned
Application No.: Unassigned	Confirmation No.: Unassigned
Filed: January 26, 2005	
For: A DATA ENCIPHERING METHOD AND ASSOCIATED CRYPTOGRAPHIC SYSTEM AND COMPONENT (As Amended)	

PRELIMINARY AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Prior to examination, kindly amend the above-captioned application as follows:

AMENDMENTS TO THE SPECIFICATION:

Please replace the title with the following amended title:

"A DATA ~~ENCRYPTION~~ ENCIPHERING METHOD[[,]] AND ASSOCIATED CRYPTOGRAPHIC SYSTEM AND ASSOCIATED COMPONENT"

Please add the following new paragraph immediately after the title appearing on page 1.

This disclosure is based upon French Application No. 02/09475, filed July 26, 2002, and International Application No. PCT/FR2003/002364, filed July 25, 2003, the contents of which are incorporated herein by reference.

Please add on a new line the following at page 1, line 6:

BACKGROUND OF THE INVENTION

Please add on a new line the following at page 6, line 19:

DESCRIPTION OF THE INVENTION

IN THE ABSTRACT:

Please add the following Abstract:

ABSTRACT

An encryption method in which a clear message (m) is formatted with a formatting function (μ), and in which the result of the formatting step is exponentiated using a public key (N, e) in accordance with the relationship $c = \mu(m)^e \bmod N$, c being an encrypted message, μ(m) being the result of the formatting step, and e and N elements of the public key. The formatting function (μ) is the PSS function. The invention is applicable to cryptography, for example of RSA type, for smart cards for instance.

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) An enciphering method comprising a step of formatting a clear message ~~in clear~~ (m) by means of a formatting function (μ), and a step of exponentiation of the result of the previous step using a public key (N, e) in accordance with the equation $c = \mu(m)^e \bmod N$, c being an enciphered message, μ(m) being the result of the formatting step, and e and N elements of the public key,

~~the method being characterised in that~~ wherein the formatting function (μ) is the PSS function.

2. (Currently Amended) A method according to claim 1, ~~characterised in that~~ wherein the formatting function μ is defined by

$\mu(m) = PSS(m) = \omega \,||\, s$, with:

m, the clear text ~~in clear~~ of k – k0 – k1 bits, r a random parameter of k0 bits, k, k0, k1 being parameters of the formatting function,

|| a concatenation function

$\omega = H(m \,||\, r)$

$s = G(\omega) \oplus (m \,||\, r)$

$\otimes$ a logic function XOR, and

H, G two hashing functions

3. (Currently Amended) ~~Use of~~ A method of enciphering a message using a probabilistic signature function ~~(PSS)~~ defined according to the standard PKCS #2 v 2.1, RSA cryptography standard as a formatting function (μ), ~~in order to effect an enciphering method~~ comprising a step of formatting a clear message ~~in clear~~ (m) by means of the formatting function (μ), and a step of exponentiation of the result of the previous step by means of a public key (N, e) in accordance with the equation $c = \mu(m)^e \bmod N$, c being an enciphered message, μ(m) being the result of the formatting step, and E and N elements of the public key.

4. (Currently Amended) A cryptographic ~~system~~ method comprising:

- a step of formatting a clear message ~~in clear~~ (m) by the probabilistic signature function ~~(PSS)~~, and then:

- if an enciphering of the clear message ~~in clear~~ (m) is required, a step of exponentiation of the result of the formatting step by means of a first key (N, e) in accordance with the equation $c=\mu(m)^e \bmod N$, c being an enciphered message, μ(m) being the result of the formatting step, and e and N elements of the first key, or

- if a signature of the clear message ~~in clear~~ (m) is required, a step of exponentiation of the result of the formatting step by means of a second key (N' d') in accordance with the

equation $s = \mu(m)^{d'} \bmod N'$, s being a signed message, $\mu(m)$ being the result of the formatting step, and d' and N' elements of the second key.

5. (Currently Amended) A ~~system~~ method according to claim [[3]] 4, in which the first key and the second key are respectively a public key of a first pair of keys and a private key of a second pair of keys.

6. (Currently Amended) A ~~system~~ method according to claim [[4]] 5, in which the first pair of keys and the second pair of keys are identical.

7. (Currently Amended) A ~~system~~ method according to ~~one of claims 4 to 6,~~ claim 4, in which the enciphering is of the RSA type.

8. (Currently Amended) An electronic component comprising a programmed ~~means~~ processor for implementing an enciphering method according to ~~one of claims 1 to 2~~ claim 1, the programmed ~~means~~ processor comprising ~~in particular~~ a central unit and a program memory.

9. (Currently Amended) An electronic component comprising a programmed ~~means~~ processor for implementing a cryptographic ~~system~~ method according to ~~one of claims 4 to 7~~ claim 4, the programmed ~~means~~ processor comprising ~~in particular~~ a central unit and a program memory.

10. (Currently Amended) A chip card comprising an electronic component according to ~~claim 7 or~~ claim 8.

11. (New) A chip card comprising an electronic component according to claim 9.

REMARKS

By way of the foregoing amendments, the specification has been amended to incorporate the priority information and the title headings. The title has been amended to conform to the English language translation. The Abstract has been added to conform the application to the corresponding PCT Application No. PCT/FR2003/002364. Claims 1-10 have been amended to delete multiple dependencies, and to otherwise conform with conventional U.S. format. New claim 11 has been added. No new matter has been introduced by these changes.

It is requested that the application be examined on the basis of the specification, the title, the Abstract, and the claims as amended.

Early and favorable consideration with respect to this application is respectfully requested.

Should any questions arise in connection with this application, the undersigned respectfully requests that he be contacted at the number indicated below.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: January 26, 2005

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620